Volume 7, Issue 4, April 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Modeling Trust Management among Cloud Entities

Akanksha Bali
Assistant Professor, Dept of CSE, YCET, Jammu and Kashmir, India

Malvika Ashok
Assistant Professor, Dept of CSE, YCET, Jammu and Kashmir, India

Mohammed Sarfaraz
Dept of CSE, Amity University, India

Abstract- Earlier the term trust was used as a synonym with security, but nowadays it has drawn attention of several enterprises. Several research from the fields of IT and computer sciences are extensively going on. Through this paper a trust evaluation model has been devised based on the evidence. The evidence is based on the interaction and uses the rule of Dempster-Shafer. This model evaluates both the cloud entities i.e. Cloud User and the cloud service providers. The proposed trust model is basically divided into two distinct cloud roles; cloud service provider and cloud user. Our model trust evaluation model will evaluate the each entity and give way for the respective trust values. The cloud user evaluation model will extract the user data collected from the cloud service providers. And based on the feedback the trust value is generated. The trust value generated are used in combination using D-S rule to find the whether it is credible entity or not.

Keywords- Cloud Providers, Cloud Users, Trust Evaluation

I. INTRODUCTION

Although Cloud computing exists long back, there is no proper definition of it, Cloud computing can be termed as a pool that consist of physical hardware, application and system software providing services that can be accessed through the "cloud". These resources can be accessed anywhere and anytime [2]. When this concept came to existence, it was very promising and was expected to take over the whole internet. The main reason was security, user or enterprise don't want to give up the data control which they usually have as they do in traditional in-house organizational infrastructure. Disclosure of data, loss due to physical damage, or crash in cloud computing services are major risk that cause distrust on the cloud entities.

Compared to traditional technologies, cloud gives a lot of advantages; such as large pools of resource are available almost every time and everywhere, the clouds are completely heterogeneous in nature [1]. The survey by Gartner shows different factors affecting the trust among cloud entities, i.e. Cloud user and Cloud Provider [4].

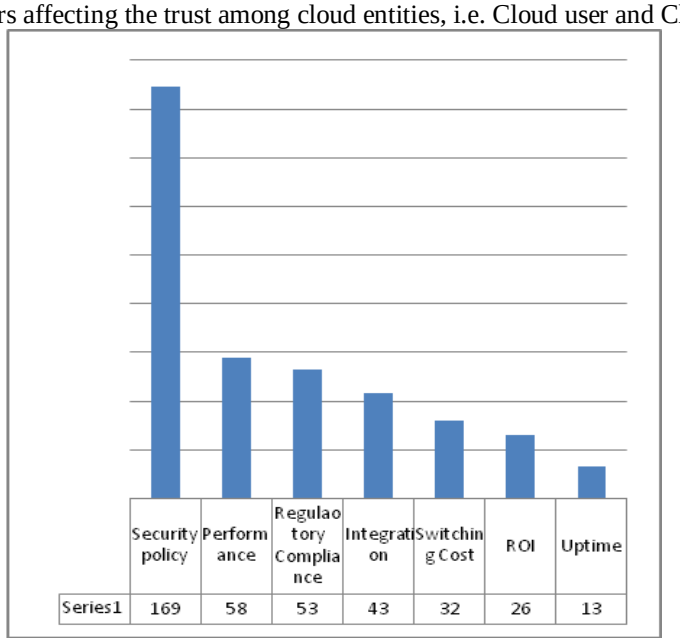

Figure 1: survey

Factors like transparency, migration rules, software compliance and data storage locations are often overlooked, but contribute to user's confidence to a large extent. Sarfaraz et al in his paper have pointed several factors and pointed out the flaws in existing methodologies used to evaluate trust in cloud entities. SLAs are an important weapon for legal fight-back for the user in case os service denial or lack in quality of services promised, but it is only applicable once both entities comes to terms[3].

II. RELATED RESEARCH

In Cloud computing environment, establishing trust and its evaluation is a tedious task due to the variedly inconsistent, intangible behavior of trust. Trust evaluation is integral aspect and various enterprise and organizational groups are currently working on evaluating the trust models. Several researchers have proposed different models to evaluate trust to resolve this issue; however a lot of questions remain unanswered.

Sarfaraz et al. have pointed various parameters and attributes for establishment of trust in cloud computing. Factors such as Service level agreement (SLA), Accreditations, and Ratings play important role in establishing trust in cloud computing. Apart from these parametric boundaries of trust are defined by the parametric aspect like transparency, SLA, policies, security and privacy, authentication and access control, portability, performance and customer support discussing the limitations of each. The problem with SLAs is that there is no standardization of SLA, the cloud service provider ay quotes the policies by discussing with the Cloud user. Generally the cloud user doesn't pay heed to minute details like authentication policies and lock ins etc. Accreditations done by the cloud service provider is that there is no overall accreditation services, small and medium enterprise would not spend money to acquire distinct parameters accreditation. Self assessment questionnaire refers to the questionnaire which the cloud service provider fills out so that the cloud user can have the proper idea that what the cloud service is all about, but in the self assessment questionnaire, the honesty of the cloud service providers are always kept in doubt [3].

Alhamad et al. have proposed a trust estimation model that uses SLA-based trust evaluation of CSP that comprises of SLA-agent, Cloud user and Cloud services provider (CSP). The core of the model is SLA-agent that is responsible for designing the SLA parameters and negotiating the SLA with CSP. The SLA agent being the crux of the model, have the ability to deal with the Cloud user and the Cloud service Providers for planning the policies and negotiating with them. The problem with the proposed system is it takes only SLA for establishing trust, which doesn't hold true [4]. The Cloud User can rightfully ask for the required services and have legal document (SLA) to back up in case of service unavailability, for that a measure to evaluate the factors of services given must established and evaluated [5].

Talal H. Noor et al, in his paper went on to propose a new type of services called trust as a services (TaaS), he proposed a framework which evaluates Cloud User and Cloud service providers. The evaluations are done by layer called TMSL, which are based on the customer feedback and the cloud Service providers as well. They particularly proposed the cloud consumer's *Capability* and the *Majority Consensus* factors for evaluating the trust of cloud services. This model also checks the credibility of the model through collection of trust feedback and its assessment, the credibility model of the TMS(Trust Management Service) layer then assess the credibility of each user whether they are malicious user giving the vague data resulting in change in trust value creating a integrity issues of the cloud systems. In addition to the given features the TMS (Trust Management Service) layer TMS assess the trust feedback and stores the data to be managed as well for future use [6].

Conner et al proposed a framework for trust evaluation system for decentralized network. This system works as a SOA (Service Oriented Architecture) that supports Cloud Service view, offering a various evaluation metrics that allow evaluation of Cloud Users [7].

Malik and Bouguettaya proposed reputation evaluation techniques for decentralized networks, the proposed architecture like previous framework supports varied metrics like credibility rating, past rating history etc. But unlike the previously defined framework it doesn't take the users feedback. Thus, eliminating limitations of previously defined architectures [8].

Wenjuan Li et al, have proposed a trust model to resolve security issues in cloud computing allowing the providers to select from a pool of providers giving the required services, this model uses the recommendation for the type of cloud services like computation or storage. The model also analyses the identity and behavior identification of the user [9].

Chenhao Qu and Rajkumar Buyya, have proposed an trust assessment model which uses hierarchical (FIS) fuzzy inference system for Infrastructure as a Services (IaaS) for selecting the type of services. This model works in four distinct parts, (1) Web interface model: which ask the user to give their functional requirements. (2) Service discovery: based on the requirements of the user, the service discovery model extracts the best suited services from the repository which is used to store the IaaS services information. (3) the trust assessment part is the core of the model, this assess the trusted or untrusted service providers based on their previous records, the cloud user or brokers then based on these records select the service providers. (4) the benchmark services of this model provides the assessment of the cloud services by continuously providing dummy data to check the credibility of each cloud service providers, hence no external third party assessment of the service providers are not needed. This model gives two distinct advantages, first the cloud user are given the option to select the service provider as per their need. Secondly, it eases the IaaS selection process whether it is for naïve or experienced user using the Fuzzy System, the maximum limit and minimum limit shows the degree of parameters the cloud service provider can handle, thirdly this model enhances the cost-efficiency and promotes the businesses of the cloud [10].

Haiyang Ding et al, proposed a trust model based on the theory of evidence. This model limits the adequacy of an entities requirement for evaluating trust. The authors have proposed a method that dynamically allocates trust weights (Direct or indirect trust) and generates a trust value through a mathematical calculation model. It also put forth an way to avoid malicious evaluation of Cloud Service Providers so that incorrect trust value is generated. But the problem with this model is evidence are based on their past records and current as well, but in case of new cloud service provider there is no way that can be evaluated to generate evidence [13].

Although we performed a literature research on the keywords trust model, cloud computing, SLA, Reputation, Direct trust etc a lot of papers exists but only a few implementations have been made, thus there is a lot of issues remain unanswered [14]. Several authors have devised an different methods to provide cloud services to only trusted service providers based on their previous performances and their feedbacks but each of them has its own flaws, we through this paper have tried to cover maximum parameters so that an the cloud entities such as cloud service provider and cloud user can evaluate themselves with minimum faults.

III. PROPOSED TRUST EVALUATION MODEL

Trust have been most effective means to enhance the businesses, and the security mechanism implied on the distributed systems can be alternatively done through the trust management models. Through this research we aim to enhance the cloud's QoS parameters in cloud, which benefits not only the Cloud customers but also with respect to the Cloud Service Providers (CSP) are modeled using the Trust Management module. The research also aims to enhance the services by allowing the user gain insights of the working of cloud service providers (CSP).

IV. PROTOCOL FOR TRUST EVALUATION MODEL

In this paper we have used the trust value based on the interaction's evidence. Here each interactions are marked as evidence and are stored in the set E. The Set E is then can be further marled as α for positive interaction, β for negative interaction and finally ∏ for uncertain interaction. At time T the interaction between the entity I and the entity j can be marked as $\alpha^t_{i,j}$ for the positive interaction, $\beta^t_{i,j}$ for negative interaction, and $\prod^t_{i,j}$ for uncertain interaction.

Here we have used the Dempster-Shefer rule, since the Dempster-Shefer evidence theory gives the probability of the certainty. Unlike the Bayes theory, the Dempster-Shefer theory gives better probability value.

The trusted, untrusted and uncertainty value can be distinguished by Δ= {t,-t}, where 2^{Δ}={f,{t},{-t},{t,-t} } , according to the DS rule, where f represent the trust, distrust and finally the uncertainty.

For the time t, the entity i evaluate the trust factor of entity j as

$dt^t_{i,j}$= { $dm^t_{i,j}${t}, $dm^t_{i,j}${-t}, $dm^t_{i,j}${t, -t}}

for the time t= t_0 , the $dt^0_{i,j}$= {0,0,1}, and the $dm^t_{i,j}${x} can be defined as

$$dmti,j\{t\} = u \text{ x } dm(t-1)i,j\{t\} + (1-u) + \frac{\alpha t\, i,j}{\alpha t\, i,j + \beta\, t\, i,j + \prod t\, i,j}$$

$$dmti,j\{-t\} = u \text{ x } dm(t-1)i,j\{t\} + (1-u) + \frac{\beta t\, i,j}{\alpha t\, i,j + \beta\, t\, i,j + \prod t\, i,j}$$

$dm^t_{i,j}${t,-t}= 1 - $dm^t_{i,j}${t}- $dm^t_{i,j}${-t}

Here u belongs to the weight factor, it can vary from 0 to 1. The weight factor $dm^t_{i,j}${x} also takes the past value into account and any changes is carried forward to the next values of trust [11].

The D-S theory states that each evidence has a degree of the belief lying between 0 and 1:

A. Where 0 refers that there is no support to the fact
B. Where 1 states that there is full support to the fact

V. EXPERIMENTAL EVALUATION

To evaluate the proposed model, we have simulated our models through the web application, to evaluate Cloud Service Provider and Cloud users.

Different parameters are taken of the cloud environments, such as Cost, Scalability and security. Based on ups and downs of these parameters, this made predicts the trust values dynamically.

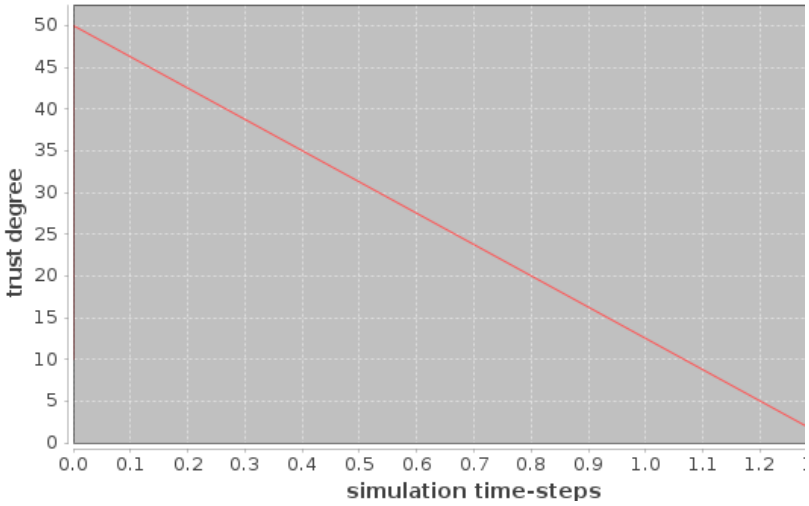

Figure 2. Trust degree

The trust degree degrades if the factors like scalability value and security type changes. In our experiment, the values of parameters decreased, with time based on it the values of trust degree also consistently decreases.

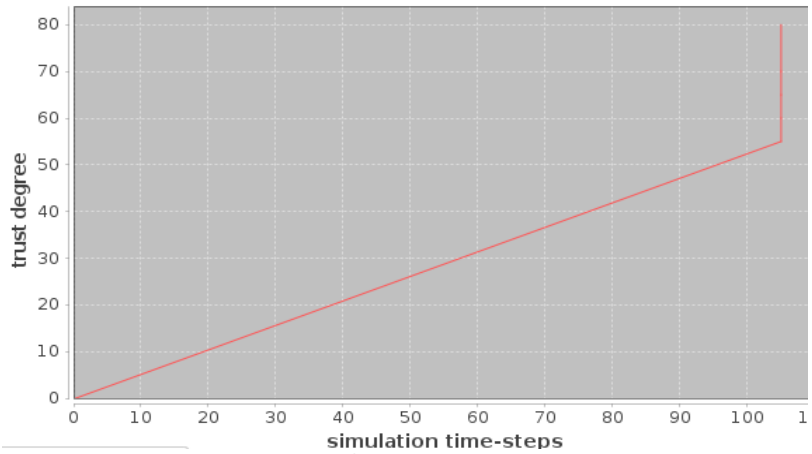

Figure 3. Untrust Degree

In our experiment, the values of parameters decreased, with time based on it the values of trust degree also consistently decreases. The untrust degree classify the malicious users, who can give misleading feedback attack where dishonest recommenders attempt to corrupt the reputation of good entities.

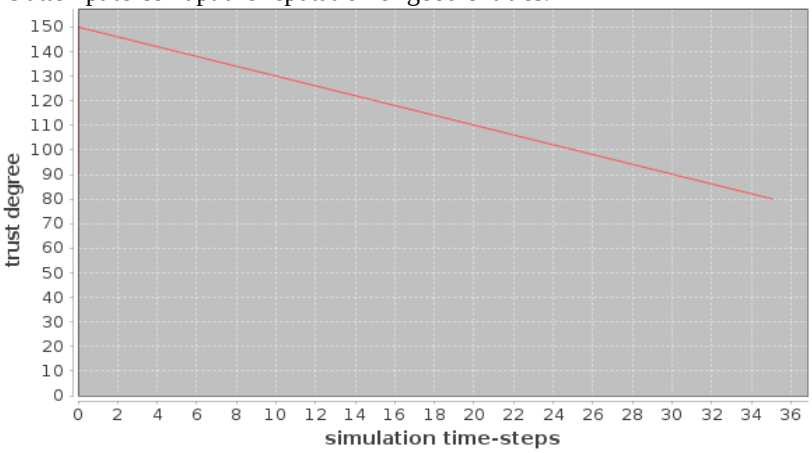

Figure 4. Uncertainty Degree

The uncertainty degree graph reflects the those CSPs which cannot be classified, in our experiment some values like which changes fast so that the trust values generated vary so much that it is difficult to predict the trust or untrust degree of the CSPs.

In our experiment values given, the parameters or factors of cloud environment slows down with time. Thus the trust degree value degree. And the untrust degree increases overtime as the parameters decreases overtime showing decreasing confidence over time. The uncertain degree and it burst abruptly at once. The uncertainty degree value here increases slowly, initially thus for sometime it can be predicted the trust and untrust degree.

We have integrated all these values to generate the overall trust values of all the cloud providers. This integrated form can be stated as

$dt^t_{i,j}(A) = dt^t_{1,j}(A) \pm dt^t_{2,j}(A) \pm \ldots\ldots \pm dt^t_{n,j}(A)$

where n=1,2,3….m, $A \epsilon 2^{\Omega}$

Based on the above equations we have generated graphs on trust.

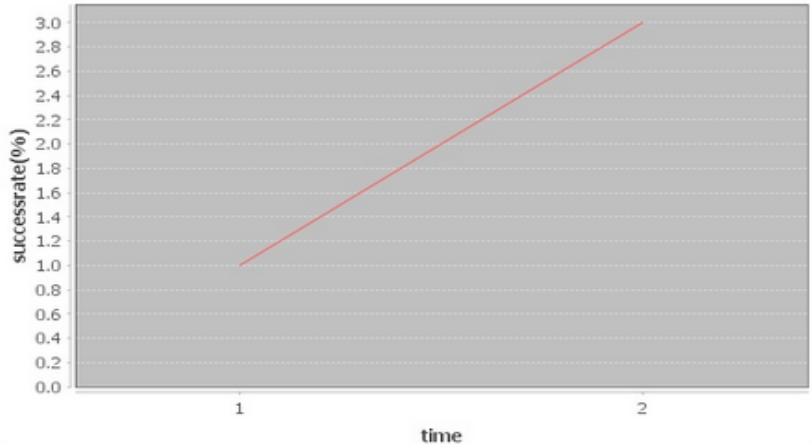

Figure 5. Trust success rate

Here the success rate defines the successful generation of trust and distrust values. The graphs here shows the positive result as it successfully generated the distrust values and the trust values from the parametric values given.

VI. CONCLUSIONS

Trust was considered anonymous with the cloud security, but it is much more than that. Trust integrates the security, performance resource and all the aspect which on which the working of cloud depends. Through this paper we have implemented a evidence based implementation model for cloud computing environment. The proposed model have the following advantages: firstly, it is easy to implement and easier to execute, the complexity of this model is O(n) where n is the number of CSPs available. Secondly, the graphs shown in this model are based on timelines, so it provides good analysis of the given data. Thirdly, the trust values are calculated dynamically based on their behavior, this behavior are calculated based on the D-S rule or simply the evidence theory.

VII. FUTURE SCOPE

Although we have implemented working on the cloud assessment of the trust, this paper only uses the encryption standards for security. Although it is most important step for implementing security, but the security features are much more extended to much more than what has been done. Security itself is a vast parameter; one can enhance the security by several ways by implementing the issues like cryptography, network security, VM vulnerabilities etc. Customer's feedback must also be considered in evaluation of trust.

REFERENCES

[1] Cloud Security Alliance. (2009). "Security Guidance for Critical Areas of Focus in Cloud Computing".
[2] National Institute of Standard and Technology (2010). "NIST Cloud Computing Standards Roadmap"
[3] Raj. G, Sarfaraz. M, "Survey on Trust establishment in Cloud computing ", IEEE, Confluence The Next Generation Information Technology Summit (Confluence), 2014
[4] Kanwal A. , Rahat M. and Shibli M. A., "Evaluation and Establishment of Trust in Cloud Federation", ACM 8th International Conference on Ubiquitous Information Management and Communication, pp. 1-5, 2014
[5] Alhamad, M, Dillon, T, Chang E, "SLA-Based Trust Model for Cloud Computing", IEEE International Conference on, pp. 321 - 324, 2010.
[6] Talal H, Quan Z. "Trust as a Service: A Framework for Trust Management in Cloud Environments", ACM 12th international conference on Web information system engineering, pp. 314–321, 2011
[7] Conner, W., Iyengar, A., Mikalsen, T., Rouvellou, I., Nahrstedt, K.: "A Trust Management Framework for Service-Oriented Environments", 18th international conference on World wide web, pp. 891-900, 2009.
[8] Malik Z. and Bouguettaya A, "RATEWeb: Reputation Assessment for Trust Establishment among Web services", ACM The VLDB Journal - The International Journal on Very Large Data Bases, pp. 885-991, 2009.
[9] Lee. W, Ping. L "Use Trust Management Module to Achieve Effective Security Mechanisms in Cloud Environment", International Conference on Electronics and Information Engineering, IEEE, 2010.
[10] Chenhao Q and Rajkumar Buyya, "A Cloud Trust Evaluation System using Hierarchical Fuzzy Inference System for Service Selection", IEEE 28th International Conference on Advanced Information Networking and Applications, pp. 850-857, 2014.
[11] Guan J. ,Bell. D. , Lesser V. , "Dempster-Shafer theory and rule strengths in expert systems" IEEE colloquium on reasoning under uncertainty, pp 61-63, 1998.
[12] Xiaonian W. , Runlian Z. , Bing Z. and Shengyuan Z. ," A trust evaluation model for cloud computing", Information Technology and Quantitative Management, Science Direct, pp. 1170-1177, 2013.
[13] Haiyang D, Xiguang L and Changqing G, "Trust Model Research in Cloud Computing Environment", International Symposium on Computers & Informatics (ISCI 2015), pp 1089-1096, 2015
[14] Buyya, R, Chee. S, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", Future Generation Computer Systems, Science Direct, 2009.
[15] Wang D. , Tim M. , Yang L. , and Zhang J. , "Towards Robust and Effective Trust Management for Security: A Survey", IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications , pp. 511-518, 2014
[16] Josang G. "Challenges for robust trust and reputation systems" 5th International Workshop on Security and Trust Management, Springer, pp. 406-413, 2009

